

# Science on the Hill: For cybersecurity, in quantum encryption we trust

September 13, 2015

## [Science on the Hill: For cybersecurity, in quantum encryption we trust](#)

by Raymond Newell

Current encryption methods are based on the difficulty of finding the right numbers in the key. The Achilles' heel is that all encryption requires unpredictable, unguessable random numbers and computers do not (generally) do unpredictable things. Large data centers, like those used by online shopping sites, aren't good at generating truly random numbers in sufficient quantity to offer bulletproof encryption. So to provide truly secure data communications, we need a reliable source of unpredictable numbers that aren't generated by a set of mathematical operations, or algorithm.

Los Alamos National Laboratory has specialized for decades in security and pushed the limits of computing. With that background, it's only natural that we made it our business to improve data security with a solution from outside traditional computing. From the physicist's point of view, the only true unpredictability comes from quantum mechanics. That's why Los Alamos physicists developed a quantum random number generator and a quantum communication system, both of which exploit the weird and immutable laws of quantum physics to improve cybersecurity.

This article first appeared in the [Santa Fe New Mexican](#).

Managed by Triad National Security, LLC for the U.S Department of Energy's NNSA